Short Descriptions

Security Package Deployment Timeline Items

Logging and Monitoring

Logging and monitoring reduces the risk of attackers hiding their malicious actions while trying to compromise and control systems and applications, steal information or destroy data. In most security breaches the evidence of the breach was in log files which were difficult to retrieve and review. Having a centralized logging environment allows for faster identification and response.

Vulnerability Management

Tools used to find security flaws or weaknesses in state systems and applications. Vulnerability management tools enable the state to find and mitigate security flaws before an attacker exploits them as a means to compromise and control systems and applications.

Forward Proxy

A forward proxy allows for protected web browsing by users by reducing the risk of a user browsing to a malicious website or downloading malicious software.

Penetration Testing

Penetration testing involves mimicking the actions of attackers to target and exploit an agency to determine what kind of access, data loss, and control and attacker can gain.

Web Application Firewall

Web application firewalling reduces the risk of compromise by detecting and blocking attacks to the most targeted threat vector of the application.

Mobile Device Management

Tools used to monitor and control mobile devices including smartphones and tablets. Mobile device management enables the state to secure and control the data accessed by mobile users.

Tiger/Audit Team

Personnel dedicated to the task of assisting agencies implement security controls to increase their security posture and reduce the risk of compromise to the entire state enterprise.

Discovery Tool

A discovery tool identifies and reports on unauthorized software and devices on systems or networks to reduce the risk of vulnerable systems being installed and targeted by attackers for compromise.

AntiVirus

Anti-Virus reduces the risk of malicious software being installed and leveraged on a user’s workstation to capture data or compromise other systems in the state network.

Data Loss Prevention

Data loss prevention detects and blocks protected information such as health and banking data from being publicly released.